**Valutazione del rischio e misure di sicurezza per i dati personali**

La valutazione dei rischi qui svolta è stata redatta in conformità con le indicazioni fornite dall’ENISA (European Union Agency for Network and Information Security) nell’elaborato “Handbook on Security of Personal Data Processing”.

**Step 1: Definizione dell'operazione di trattamento e del suo contesto**

|  |
| --- |
| **1. Cos’è l'operazione di trattamento dei dati personali?** |
| GESTIONE ALUNNI  (sin dal momento della presentazione della domanda di iscrizione) |

|  |
| --- |
| **2. Quali sono le tipologie di dati personali trattati?** |
| **Dati comuni:**  Dati comuni “ordinari”: Dati anagrafici e contatti; Dati contabili, fiscali e finanziari (stati pagamento assicurazione/mensa/visite didattiche, etc.); Dati derivanti da tracciamenti (log); Dati audio/foto/video;  Dati comuni inerenti a situazioni speciali: Dati inerenti situazioni giudiziarie civili, amministrative, tributarie (relativi alla famiglia dello studente e a situazioni personali rilevanti ai fini dell’iscrizione, tra cui, ad esempio situazioni come divorzio/separazione, interdizioni/inabilitazioni, *etc.*); Dati inerenti al rapporto di lavoro (dei genitori o chi esercita la responsabilità genitoriale). |
| **Categorie particolari di dati:**  L'origine razziale ed etnica; Le convinzioni religiose, filosofiche e di altro genere; Lo stato di salute; Assistenza sanitaria |
| **Dati personali relativi a condanne penali e reati:**  N/A |

|  |
| --- |
| **3. Qual è la finalità del trattamento?** |
| Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi scolastici aggiuntivi e adempimento degli obblighi previsti dal D.M. 692/2017, nonché finalità organizzative a ciò strumentali (come assegnazione classe, organizzazione laboratori, *etc.*). |

|  |
| --- |
| **4. Quali sono gli strumenti utilizzati per il trattamento dei dati personali?** |
| Utilizzo di servizi ICT, Utilizzo di strumenti di office automation (Modalità elettroniche, uso sistema informativo MI (SIDI)/pacchetti locali); Gestione manuale |

|  |
| --- |
| **5. Dove avviene il trattamento dei dati personali?** |
| I Dati Personali non sono di norma oggetto di trasferimento verso Paesi terzi od organizzazioni internazionali. Tuttavia, qualora ciò dovesse rendersi necessario (anche nell’ambito dello svolgimento dei servizi forniti alla Scuola da soggetti terzi), l’eventuale trasferimento avverrà in conformità ai requisiti prescritti dalla normativa europea e quindi in presenza di condizioni tali da assicurare un livello di protezione dei Dati Personali conforme a quello richiesto dal GDPR (come, ad esempio, in forza di clausole contrattuali standard, decisioni di adeguatezza, *etc.*). |

|  |
| --- |
| **6. Quali sono le categorie di soggetti interessate?** |
| Studenti (anche minori); genitori o chi esercita la responsabilità genitoriale; Altri soggetti - persone fisiche (come, ad esempio, assistenti sociali o eventuali altri operatori delle amministrazioni locali addetti a servizi inerenti ai giovani e alle loro famiglie). |

|  |
| --- |
| **7. Chi sono i destinatari dei dati?** |
| Pubblica amministrazione; Soggetti privati (persone fisiche o giuridiche) |

**Step 2: Comprensione e valutazione dell'impatto**

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | **LIVELLO DI IMPATTO** | | |  | | --- | | **DESCRIZIONE** | |
| Basso | Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.). |
| Medio | Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.). |
| Alto | Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.). |
| Molto alto | Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.). |

|  |  |  |
| --- | --- | --- |
| **N.** | **DOMANDA** | **VALUTAZIONE** |
| **I.1.**  **Perdita di riservatezza** | **Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.** | Basso  Medio X  Alto  Molto Alto |
| **I.2.**  **Perdita dell'integrità** | **Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.** | Basso  Medio X  Alto  Molto Alto |
| **I.3.**  **Perdita della disponibilità** | **Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.** | Basso  Medio X  Alto  Molto Alto |

|  |
| --- |
| **I.1. Perdita di riservatezza**  Nell'ambito dell'operazione di trattamento specifica, l'impatto della perdita di riservatezza è considerato come **MEDIO**, in quanto in alcuni casi gli individui (studenti, minori e genitori/tutori) potrebbero sperimentare notevoli effetti negativi derivanti dalla divulgazione di determinati dati (ad esempio riguardo al comportamento dell’alunno o relativi a specifici disturbi dell’apprendimento).La perdita di riservatezza è di per sé potenzialmente idonea anche a esporre la persona e il suo nucleo familiare a condizionamenti o discriminazioni.  **I.2. Perdita dell'integrità**  L’impatto derivante dalla perdita di integrità può parimenti essere considerato come di valore **MEDIO**, in quanto la modifica non autorizzata di questi dati potrebbe ostacolare la corretta gestione del servizio scolastico con ulteriori complicazioni (ad esempio in merito alle valutazioni).  **I.3. Perdita della disponibilità**  L’impatto derivante dalla perdita di disponibilità può essere considerato **MEDIO**, dal momento che l'indisponibilità dei dati può determinare limitati inconvenienti che possono essere facilmente superati (presupponendo che siano sempre disponibili back-up, dati conservati dai gestori delle piattaforme designate responsabili del trattamento o conservate con conservazione digitale a norma e informazioni di tutti i documenti gestiti dalla scuola).  Essendo il risultato complessivo della valutazione dell'impatto il più alto identificato, l'impatto complessivo valutato risulta essere **MEDIO**.  Oltre alle ipotesi formulate nell’ambito del presente scenario pratico potrebbero verificarsi casi in cui l'impatto complessivo potrebbe essere superiore a quello appena sopra calcolato. Un esempio di tali ipotesi è quando vi sono particolari dati di alunni con condizioni di disabilità. |

**Step 3: Definizione di possibili minacce e valutazione della loro probabilità**

Domande riprese dalle indicazioni fornite dall’ENISA:

le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

* Risorse di rete e tecniche (hardware e software)
* Processi / procedure relativi all'operazione di trattamento dei dati
* Diverse parti e persone coinvolte nell'operazione di trattamento
* Settore di operatività e scala del trattamento

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A. RISORSE DI RETE E TECNICHE**   |  |  | | --- | --- | | **Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?** | Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet. | | **È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?** | Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT. | | **Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?** | La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso). | | **Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?** | Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico). | | **Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?** | Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza. | | | |
|  |  |  |

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

|  |  |
| --- | --- |
| **I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?** | Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema. |
| **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?** | Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali. |
| **I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?** | I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi. |
| **I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?** | L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni. |
| **Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?** | La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali. |

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

|  |  |
| --- | --- |
| **Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?** | Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali. |
| **Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?** | Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo. |
| **Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?** | Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo. |
| **Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?** | Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza. |
| **Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?** | Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati. |

D. SETTORE DI OPERATIVITA’ E SCALA DI TRATTAMENTO

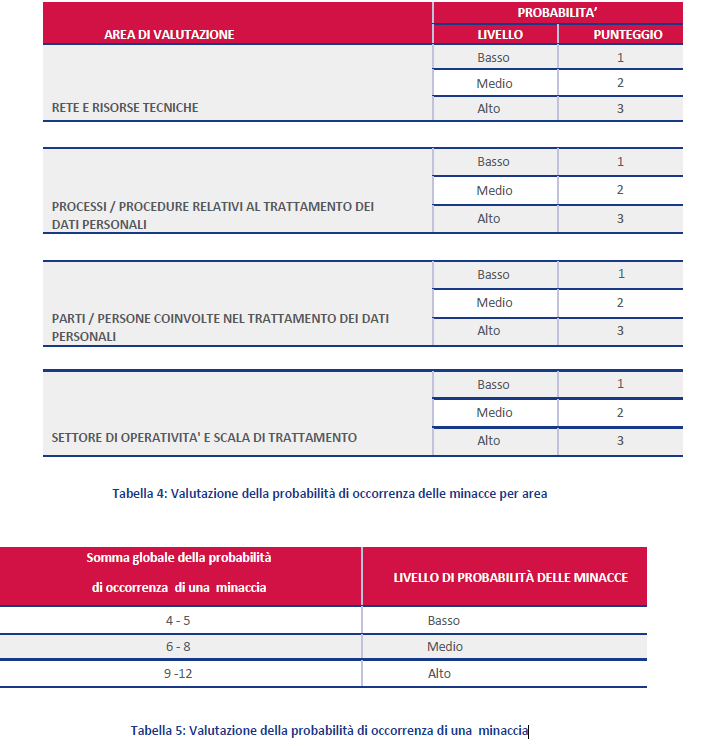
|  |  |
| --- | --- |
| **Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?** | Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell’organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile. |
| **La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?** | Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro. |
| **Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?** | Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra. |
| **Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?** | Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati). |
| **Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?** | Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza. |

|  |
| --- |
| **Risorse di rete e tecniche**: la probabilità di occorrenza delle minacce è di valore **MEDIO**, poiché il sistema è connesso alla rete internet (rete protetta da firewall) e vengono utilizzate dalla scuola, per il trattamento dei dati personali, diverse piattaforme cloud, gestite da soggetti esterni, appositamente designati responsabili del trattamento. Ad esempio i genitori accedono tramite connessione internet al registro elettronico ove vengono indicati e specificati i voti degli studenti e notizie relative alla vita scolastica. In ogni caso l’accesso avviene solo tramite credenziali fornite individualmente dalla scuola. Inoltre, vengono utilizzate best practices per impedire l'accesso non autorizzato a tali piattaforme e si dà per presupposto il loro aggiornamento. Anche il personale scolastico per poter accedere a tutte le piattaforme (attraverso le quali vengono gestiti i dati personali di studenti e genitori/tutori) deve seguire specifiche istruzioni e gli vengono fornite apposite credenziali individuali in base alle mansioni affidate personalmente. Infine l’accesso all’ambiente fisico è monitorato e le persone esterne alla scuola possono accedere ai locali solo se autorizzate. I computers della scuola possono essere utilizzati soltanto dai dipendenti della scuola appositamente abilitati e con specifica password.  **Processi / Procedure relative al trattamento dei dati personali:** La probabilità di occorrenza di una minaccia è di valore **MEDIO**, in quanto vi sono diversi soggetti che accedono alla stessa piattaforma ma con ruoli e le responsabilità definiti. Ed infatti, il personale della scuola in base al ruolo e al compito che svolge riceve le password e gli identificativi per l’accesso agli applicativi e ai programmi per la gestione amministrativa e didattica della scuola. La scuola effettua poi periodici controlli disattivando i profili e gli account del personale (e degli studenti/genitori) non più in servizio presso l’istituto. Ognuno per accedere possiede proprie password e vengano creati appositi file di log per tracciare qualsiasi attività di trattamento svolta. Si segnala altresì che i sistemi operativi gestiti dai fornitori esterni di gestionali scolastici su piattaforme cloud registrano gli event-log. Gli accessi degli utenti sono perciò monitorati e ciò è garantito dall’univocità delle credenziali assegnate ad ogni utente utilizzatore.  **Parti / Persone coinvolte nel trattamento dei dati personali:** La probabilità di occorrenza di una minaccia è di valore **MEDIO** poiché è presente più di un responsabile esterno dei dati personali (tra cui il MI per il sistema SIDI). Tutti i dipendenti che hanno accesso ai dati sono appositamente designati persone autorizzate al trattamento ed istruite. Il personale scolastico è in grado di trasferire, archiviare o elaborare dati personali della scuola. Tuttavia, si presume sia chiaramente definito a tutti i dipendenti l'uso della rete, del sistema e delle risorse fisiche. Infine l’accesso della scuola è sempre controllato e nelle ore di chiusura vengono attivati sistemi di allarme. Gli accesi agli applicativi e ai documenti informatici e/o cartelle condivise della scuola sono tutti limitati e controllati.  Inoltre, come già riportato al punto precedente, il personale della scuola in base al ruolo e al compito che svolge riceve le password e gli identificativi per l’accesso agli applicativi e ai programmi per la gestione amministrativa e didattica della scuola.  **Settore di operatività e scala/dimensione del trattamento:** la probabilità di occorrenza di una minaccia è di valore **BASSO** poiché il settore di operatività (istruzione) non è generalmente considerato soggetto ad attacchi informatici. Unici attacchi generalmente affrontati dalle scuole sono quelli che utilizzano la tecnica del ransomware. In ogni caso viene effettuato un backup periodico con conservazione sicura. Si presume che nessuna violazione dei dati personali sia mai avvenuta in passato. |

Il livello di probabilità di occorrenza della minaccia è stato definito per ciascuna delle aree di valutazione, come segue:

* Basso: è improbabile che la minaccia si materializzi.
* Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
* Alto: la minaccia potrebbe materializzarsi.

Le tabelle 4 e 5 possono quindi essere utilizzate per documentare la probabilità di occorrenza delle minacce per ciascuna area di valutazione e di conseguenza calcolare il suo valore finale.



**Step 4: Valutazione del rischio**

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilavante, la valutazione finale del rischio è possibile (Tabella 6).



|  |
| --- |
| In particolare, il rischio complessivo per lo scenario pratico qui preso in considerazione è in via generale considerato **MEDIO**.  È necessario notare che il rischio potrebbe essere diverso (ALTO) in condizioni direttamente correlate ad uno specifico trattamento di dati e influire sull'impatto o sulla probabilità di occorrenza della minaccia. |

N.B. Si precisa che i fornitori delle piattaforme (oltre al Ministero dell’Istruzione per il sistema SIDI e Pago In Rete) per lo svolgimento delle attività amministrative e didattiche sono designati responsabili del trattamento e che i servizi che offrono sono qualificati e presenti nel Cloud Marketplace di AgID